



[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

Search: ☒ The ACM Digital Library ☐ The Guide

"public key" and "private key" and "digital signature" and accoi



[Feedback](#) [Report](#)

Terms used **public key** and **private key** and **digital signature** and **account\$1** and **sender** and **receiver** and **decrypt\$3** and **transaction** and **identit\$3** and **compar\$**

Sort results by

Display results

[Save results to a Binder](#)

[Search Tips](#)

☐ [Open results in a new window](#)

Try an  
Try this

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

1 [Authentication in distributed systems: theory and practice](#)

Butler Lampson, Martín Abadi, Michael Burrows, Edward Wobber  
November 1992 **ACM Transactions on Computer Systems (TOCS)**, Volume 10 Issue 4

**Publisher:** ACM Press

Full text available: pdf(3.37 MB)

Additional Information: [full citation](#), [abstract](#), [references](#), c

We describe a theory of authentication and a system that implements it. Our theory is based on the relation between principals. A simple principal either has a name or is a communication channel with an adopted role or delegated authority. The theory shows how to reason about a principal's authority to speak for; authenticating a channel is one important application. We ...

**Keywords:** certification authority, delegation, group, interprocess communication, key distribution, role, secure channel, speaks for, trusted computing base

2 [Authentication in distributed systems: theory and practice](#)

Butler Lampson, Martín Abadi, Michael Burrows, Edward Wobber  
September 1991 **ACM SIGOPS Operating Systems Review , Proceedings of the thirteenth ACM principles SOSP '91**, Volume 25 Issue 5

**Publisher:** ACM Press

Full text available: pdf(2.33 MB)

Additional Information: [full citation](#), [abstract](#), [references](#), c

We describe a theory of authentication and a system that implements it. Our theory is based on the relation between principals. A simple principal either has a name or is a communication channel with an adopted role or delegation of authority. The theory explains how to reason about a principal's authority to speak for; authenticating a channel is one important application. We use the th ...

3 [Oblivious signature-based envelope](#)

Ninghui Li, Wenliang Du, Dan Boneh  
July 2003 **Proceedings of the twenty-second annual symposium on Principles of distributed computing**

**Publisher:** ACM Press

Full text available: pdf(874.99 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), c

Exchange of digitally signed certificates is often used to establish mutual trust between strangers in business transactions. Automated Trust Negotiation (ATN) is an approach to regulate the flow of information exchange. Previous work on ATN are based on access control techniques, and cannot handle cycles. We show that the problem can be modelled as a 2-party secure function evaluation (SFE) problem ...

4 Securing the global, remote, mobile user

Walt Curtis, Lori Sinton

March 1999 **International Journal of Network Management**, Volume 9 Issue 1


**Publisher:** John Wiley & Sons, Inc.

Full text available:  pdf(982.14 KB)

Additional Information: [full citation](#), [abstract](#), [index terms](#)


Electronic commerce is inevitable and will reshape our lives, but before true electronic commerce is necessary to secure your enterprise against outside attacks on its electronic information and private information. Copyright © 1999 John Wiley & Sons, Ltd.

5 Encryption and Secure Computer Networks

 Gerald J. Popek, Charles S. Kline


December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4

**Publisher:** ACM Press

Full text available:  pdf(2.50 MB)

Additional Information: [full citation](#), [references](#), [citations](#), [index](#)

6 Astrolabe: A robust and scalable technology for distributed system monitoring, management

 Robert Van Renesse, Kenneth P. Birman, Werner Vogels

May 2003 **ACM Transactions on Computer Systems (TOCS)**, Volume 21 Issue 2

**Publisher:** ACM Press


Full text available:  pdf(341.62 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#)

Scalable management and self-organizational capabilities are emerging as central requirements for dynamic, distributed applications. We have developed an entirely new distributed information management system that collects large-scale system state, permitting rapid updates and providing on-the-fly attribute aggregation. The application to locate a resource, and also offers a scalable way to track system state.

**Keywords:** Aggregation, epidemic protocols, failure detection, gossip, membership, publish-subscribe

7 Toward a model of self-administering data

 ByungHoon Kang, Robert Wilensky

January 2001 **Proceedings of the 1st ACM/IEEE-CS joint conference on Digital libraries**

**Publisher:** ACM Press

Full text available:  pdf(308.08 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#)

We describe a model of self-administering data. In this model, a declarative description of how to manage data is provided. Each object, either by a user or by a data input device. A widespread infrastructure of self-administering handlers are responsible for carrying out the specifications attached to the data. Typically, the system should be transferred, how it should be incorporated when it is updated.

**Keywords:** asynchronous collaboration, data access model, data management, distributed file systems, update propagation, self-administering data

8 Introduction of the asymmetric cryptography in GSM, GPRS, UMTS, and its public key infrastructure

Constantinos F. Grecas, Sotirios I. Maniatis, Iakovos S. Venieris

April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2

**Publisher:** Kluwer Academic Publishers

Full text available:  pdf(107.24 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#)

The logic ruling the user and network authentication as well as the data ciphering in the GSM architecture involves the transferring of the parameters employed in these processes, by transactions between three nodes: the mobile station (MS), the visited MSC/VLR, and the AuC, which is attached to the HLR in most cases. The GPRS

of the GSM's philosophy regarding the user/network authentication and the data ciphe ...

**Keywords:** PKIs, PLMNs, asymmetric cryptography

9 A security architecture for fault-tolerant systems

 Michael K. Reiter, Kenneth P. Birman, Robbert van Renesse  
November 1994 **ACM Transactions on Computer Systems (TOCS)**, Volume 12 Issue 4

**Publisher:** ACM Press

Full text available:  [pdf\(2.50 MB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [c](#)

Process groups are a common abstraction for fault-tolerant computing in distributed systems. V the process group into a security abstraction. Integral parts of this architecture are services tha cryptographic key distribution. Using replication only when necessary, and introducing novel rej have constructed these services both to be easily defensible against atta ...

**Keywords:** key distribution, multicast, process groups

10 Smart Cards and Biometrics: The cool way to make secure transactions


David Corcoran, David Sims, Bob Hillhouse  
March 1999 **Linux Journal**

**Publisher:** Specialized Systems Consultants, Inc.

Full text available:  [html\(22.95 KB\)](#)

Additional Information: [full citation](#), [index terms](#)

11 Computer security (SEC): Fair certified e-mail delivery

 Aleksandra Nenadić, Ning Zhang, Stephen Barton  
March 2004 **Proceedings of the 2004 ACM symposium on Applied computing**


**Publisher:** ACM Press

Full text available:  [pdf\(179.18 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [ir](#)

Communication by e-mail has become a vital part of everyday business and has replaced most Important business correspondence may require certified e-mail delivery, analogous to that pro presents a novel certified e-mail delivery protocol that provides non-repudiation of origin and n protect communicating parties from each other's false denials that the e-mail has ...

12 Verification and security: Policy-hiding access control in open environment

 Jiangtao Li, Ninghui Li  
July 2005 **Proceedings of the twenty-fourth annual ACM SIGACT-SIGOPS symposium PODC '05**

**Publisher:** ACM Press

Full text available:  [pdf\(247.72 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [ir](#)

In trust management and attribute-based access control systems, access control decisions are l identity) of the requester: Access is granted if Alice's attributes in her certificates satisfy Bob's : a policy-hiding access control scheme that protects both sensitive attributes and sensitive polici certified attribute values satisfy Bob's policy, without Bob learning any ...

**Keywords:** access control, automated trust negotiation, cryptographic commitment, cryptogra privacy, secure function

13 Digital signatures with RSA and other public-key cryptosystems

Dorothy E. Denning

 April 1984 **Communications of the ACM**, Volume 27 Issue 4

**Publisher:** ACM Press

Full text available:  [pdf\(374.39 KB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)


**Keywords:** cryptanalysis, cryptographic, hashing, homomorphism, protocol

14 [Practical byzantine fault tolerance and proactive recovery](#)

 Miguel Castro, Barbara Liskov

November 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 4

**Publisher:** ACM Press

Full text available:  [pdf\(1.63 MB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#)

Our growing reliance on online services accessible on the Internet demands highly available systems that tolerate Byzantine faults. BFT can be used in practice to implement re ...

**Keywords:** Byzantine fault tolerance, asynchronous systems, proactive recovery, state machine

15 [A secure multicast protocol with copyright protection](#)

 Hao-hua Chu, Lintian Qiao, Klara Nahrstedt, Hua Wang, Ritesh Jain

April 2002 **ACM SIGCOMM Computer Communication Review**, Volume 32 Issue 2

**Publisher:** ACM Press

Full text available:  [pdf\(301.97 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#)

We present a simple, efficient, and secure multicast protocol with copyright protection in an open environment. It can run in any open network environment. It does not rely on any security ...

**Keywords:** copyright protection, key distribution, multicast security, watermark

16 [Secret key distribution protocol using public key cryptography](#)

Amit Parnerkar, Dennis Guster, Jayantha Herath

October 2003 **Journal of Computing Sciences in Colleges**, Volume 19 Issue 1

**Publisher:** Consortium for Computing Sciences in Colleges

Full text available:  [pdf\(74.93 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#)

This paper presents the description and analysis of a protocol, which uses hybrid crypto algorithm. A 168-bit key is used to generate the secret key. This secret key is transferred with the help of public key process is accomplished by using the message digest algorithm MD5. This protocol uses mutual authentication to have to authenticate themselves via a third trusted certificate authority (CA). The ...

17 [Data integrity: The HP time vault service: exploiting IBE for timed release of confidential information](#)

 Marco Casassa Mont, Keith Harrison, Martin Sadler

May 2003 **Proceedings of the 12th international conference on World Wide Web**

**Publisher:** ACM Press

Full text available:  [pdf\(860.87 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#)

Digital information is increasingly more and more important to enable interactions and transactions. Leaking sensitive information can have harmful effects for people, enterprises and governments.

dealing with timed release of confidential information and simplifying its access once public: it is and day-to-day life. We introduce the "HP Time Vault Service", based on the emerging ...

**Keywords:** disclosure policies, identifier-based encryption, privacy, security, timed-release, we

18 Escrow services and incentives in peer-to-peer networks

 Bill Horne, Benny Pinkas, Tomas Sander  
October 2001 **Proceedings of the 3rd ACM conference on Electronic Commerce**

**Publisher:** ACM Press

Full text available:  pdf(265.69 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [c](#)

Distribution of content, such as music, remains one of the main drivers of P2P development. Such receiving a lot of attention from the content industry as a viable business model for P2P content such services face is that users may choose to redistribute content outside the community of such piracy. Digital Rights Management (DRM) systems typically employ tamper resistance to ...

19 A secure infrastructure for service discovery and access in pervasive computing

Jeffrey Undercoffer, Filip Perich, Andrej Cedilnik, Lalana Kagal, Anupam Joshi  
April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2

**Publisher:** Kluwer Academic Publishers

Full text available:  pdf(308.34 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [c](#)

Security is paramount to the success of pervasive computing environments. The system presents a secure and security infrastructure that goes far in advancing the goal of anywhere-anytime computing, and utilizes services in heterogeneous networks. We provide a service registration and discovery of service management. The system is built upon a simplified Public Key Infrastructure to ...

**Keywords:** distributed services, extensible markup language, pervasive computing, security, s

20 Research track paper: Anonymity-preserving data collection

 Zhiqiang Yang, Sheng Zhong, Rebecca N. Wright  
August 2005 **Proceeding of the eleventh ACM SIGKDD international conference on Knowledge Discovery and Data Mining**

**Publisher:** ACM Press

Full text available:  pdf(817.67 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [ir](#)

Protection of privacy has become an important problem in data mining. In particular, individuals' data, frequently resulting in individuals either refusing to share their data or providing incomplete collection can affect the success of data mining, which relies on sufficient amounts of accurate data. Random perturbation and randomized response techniques can provide some help ...

**Keywords:** anonymity, data collection, data mining

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright  
[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)

## EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2	"public key".clm. and "private key".clm. and "digital signature".clm. and account\$1.clm. and sender.clm. and receiver.clm. and decrypt\$3.clm. and transaction.clm. and identit\$3.clm. and compar\$3.clm. and database.clm. and associat\$3.clm. and validat\$3.clm.	USPAT	OR	OFF	2006/04/04 07:40
L2	111	"public key" and "private key" and "digital signature" and account\$1 and sender and receiver and decrypt\$3 and transaction and identit\$3 and compar\$3 and database and associat\$3 and validat\$3	USPAT	OR	OFF	2006/04/04 07:41
L3	316	"public key" and "private key" and "digital signature" and account\$1 and sender and receiver and decrypt\$3 and transaction and identit\$3 and compar\$3 and database and associat\$3 and validat\$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/04/04 07:42
L4	2924	713/176 or 713/170	US-PGPUB; USPAT	OR	OFF	2006/04/04 07:42
L5	3926	713/182 or 380/282 or 380/285 or 705/64 or 705/67 or 705/75 or 726/1 or 726/36 or 380/229 or 713/156 or 713/175 or 902/2	US-PGPUB; USPAT	OR	OFF	2006/04/04 07:46
L6	6175	5 or 4	US-PGPUB; USPAT	OR	OFF	2006/04/04 07:46
L7	70	6 and 3	US-PGPUB; USPAT	OR	OFF	2006/04/04 07:47